

United States District Court
STATE AND DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA

V.

STEVEN MICHAEL BORGAN, JR.

CRIMINAL COMPLAINT

Case Number: 11-mj-212 (JJK)

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about July 13, 2011, in Washington County, in the State and District of Minnesota, the defendant knowingly distributed any visual depiction using any means and facility of interstate and foreign commerce and that has been mailed, and has been shipped and transported in and affecting interstate and foreign commerce, and which contains materials which have been mailed and so shipped and transported, by any means including by computer, the production of which involved the use of a minor engaging in sexually explicit conduct and which visual depiction was of such conduct, including, but not limited to, the following computer image files: 0_10649900_1163577995.jpg, 1121732131663.jpg, and baby cum.jpg in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(b)(1).

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

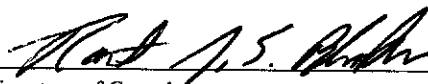
Sworn to before me, and subscribed in my presence,

7/26/11

Date

The Honorable Jeffrey J. Keyes
UNITED STATES MAGISTRATE JUDGE

Name & Title of Judicial Officer


Signature of Complainant
Robert J.E. Blackmore
FBI

St. Paul, MN

City and State


Signature of Judicial Officer

SCANNED

JUL 27 2011

U.S. DISTRICT COURT ST. PAUL

STATE OF MINNESOTA)
) ss. AFFIDAVIT OF ROBERT J.E. BLACKMORE
COUNTY OF RAMSEY)

I, Robert J. E. Blackmore, being duly sworn, hereby depose and say:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for over ten years. I am currently assigned to the Minneapolis, Minnesota, Division of the FBI and work on the Minnesota Cyber Crime Task Force. I have received specialized FBI training in both the investigation of computer and computer-related crimes and crimes involving the sexual exploitation of children. As a member of the Cyber Crime Task Force, my responsibilities include the investigation of various criminal offenses involving computers, computer networks, and the Internet, including the investigation of crimes involving the sexual exploitation of children. While employed by the FBI, I have participated in numerous investigations in which I have collected evidence in an electronic form.

2. This affidavit is based on my training, experience, personal knowledge and observations in this investigation; upon my discussions with other law enforcement officers and agents involved in this investigation; and upon my review of official reports submitted in relation to this investigation. Further, this affidavit contains information to support probable cause but is not intended to convey facts of the entire investigation.

3. This affidavit is made for the purpose of establishing probable cause in support of a federal arrest warrant and therefore contains only a summary of relevant facts.

4. On October 29, 2010, your affiant, using a computer connected to the Internet, launched a publicly available P2P file sharing program from the Minnesota Cyber Crime Task Force. I then connected to the file sharing program with a username that I had created and was indicative of a person with a sexual interest in children. I then sent "friend" invitations to several usernames who had appeared on the friends lists of other users who were found to be involved in the sharing or trading of child pornography. The usernames to whom the invitations were sent were known to have used Internet Protocol addresses ("IP addresses") that had resolved to the State of Minnesota.

5. One of the usernames that I sent an invitation to was "Sisterskids." Sisterskids had previously used different IP addresses that had resolved to two different Internet Service Providers. Subscribers to these IP addresses were located in Faribault, Minnesota, and Minneapolis, Minnesota.

6. On November 3, 2010, I observed that the username Sisterskids had accepted the previously-sent invitation.

7. On three occasions in November 2010, I downloaded image and video files directly from Sisterskids. Upon reviewing the downloaded image and video files, based on my training and experience, I believed that the majority of them depicted child pornography. Several of these files were matches to identified

victims of child sexual exploitation. Results from an administrative subpoena sent to Comcast revealed that on each of these three occasions, the IP address of Sisterskids' computer was assigned to an account registered to E.S. at a known residential address in Minneapolis, Minnesota.

8. On two occasions in December 2010, I downloaded image files directly from Sisterskids. Upon reviewing the downloaded image files, based on my training and experience, I believed that the majority of them depicted child pornography. Several of these files were matches to identified victims of child sexual exploitation. Results from administrative subpoenas sent to Mediacom revealed that on both of these occasions, the IP addresses of Sisterskids' computer were assigned to an account registered to C.N. at a known residential address in Boone, Iowa.

9. As the username Sisterskids was now utilizing IP addresses that resolved to Mediacom in Boone, Iowa, I provided the above information to the Omaha, Nebraska office of the FBI, which has jurisdiction over the State of Iowa.

10. On January 27, 2011, Task Force Officer SA Robert Larsen of the Iowa Department of Criminal Investigation served a federal search warrant upon the known residential address associated with the Mediacom account registered to C.N. in Boone, Iowa.

11. Two males were residing at this apartment and were interviewed by SA Larsen. As a result of these interviews, SA Larsen determined that the Internet connection from Mediacom at this residence was an open, unsecured wireless network at the time

the downloads of child pornography were made by your affiant. SA Larsen further determined that neither of the individuals residing at the residence appeared to be responsible for the child pornography. A forensic preview of computers in this residence showed no evidence connected to the child pornography that your affiant downloaded.

12. On January 28, 2011, FBI SA James Zajac, using a computer connected to the internet, launched a publicly available peer-to-peer file sharing program from an FBI office located in Philadelphia, Pennsylvania. SA Zajac queried his network of friends and observed that an individual with the user name Sisterskids was logged onto the network. SA Zajac downloaded 40 images from Sisterskids' computer and determined that all 40 images depicted child pornography. Several of these files were matches to identified victims of sexual exploitation. Results from an administrative subpoena sent to Mediacom revealed that at the date and time of the downloads, the IP addresses of Sisterskids' computer was assigned to an account registered to A.D. at a known residential address in Boone, Iowa.

13. On February 9, 2011, SA Larsen interviewed A.D. at her apartment in Boone, Iowa. During this interview, it was determined that the Internet connection from Mediacom at A.D.'s residence is an open, unsecured wireless network, and was at the date and time when child pornography images were downloaded by SA Zajac. SA Larsen further determined that none of the individuals residing at

A.D.'s residence appeared to be responsible for the illicit activity connected to this case.

14. A.D. consented to leave her Internet connection open and unsecured in order for law enforcement to monitor the use of her wireless access point.

15. On February 9, 2011, at approximately 6:19 p.m., I received information that the username Sisterskids was online and that this user was connected from the Mediacom IP address 173.26.191.107. Additionally, this user was assigned the private internal IP address of 192.168.2.16. A subpoena served on Mediacom for the IP address 173.26.191.107 for this date and time showed that it was accessed by A.D.'s account at her residence in Boone, Iowa.

16. On February 9, 2011, A.D. provided SA Larsen screen captures from 7:18 p.m. and 9:06 p.m. One of the host names using her wireless access point was identified as "Steven-PC." This host name was utilizing the private IP address of 192.168.2.16, the same private IP address that was assigned to Sisterskids in paragraph 15 above. The MAC address connected to this host name and private IP address was identified as 70:F1:A1:90:76:80.

17. On February 11, 2011, at approximately 4:01 p.m., I received information that the username Sisterskids was online and that this user was connected from the Mediacom IP address 173.26.191.107. Additionally, this user was assigned the private internal IP address of 192.168.2.11.

18. On February 11, 2011, A.D. provided SA Larsen a screen capture from 5:32 p.m. One of the host names using her wireless access point was identified as "Steven-PC." This host name was utilizing the private IP address of 192.168.2.11, the same private IP address that was assigned to Sisterskids in paragraph 17 above. The MAC address connected to this host name and private IP address was identified as 70:F1:A1:90:76:80.

19. On March 5 and 6, 2011, I received information that the user Sisterskids was online from IP address 71.220.40.32. Results of an administrative subpoena to Qwest Communications revealed that at the dates and times when Sisterskids was online, this IP address was assigned to a Perkins Restaurant in Cottage Grove, Minnesota.

20. On March 7, 2011, I downloaded image and video files directly from Sisterskids. Upon reviewing the downloaded image and video files, based on my training and experience, I believed that the majority of them depicted child pornography. Three of these files were matches to identified victims of child sexual exploitation. At the date and time of the downloads, the IP address of Sisterskids' computer was the same IP address that was previously determined to be assigned to Perkins Restaurant in Cottage Grove, Minnesota.

21. In addition to the images of child pornography that I downloaded from Sisterskids on March 7, 2011, I also downloaded several non-pornographic images. Among these images were the following:

- a. "me and my niece.bmp" which depicts a white adult male sitting beside a white minor female.
- b. "me.bmp" which depicts a person riding a blue motorcycle with the numerals "411" on it. The image has the text "MNracing.com" on it.
- c. "XXXXXX birthday.bmp" which depicts a girl who appears to be a teenager holding a birthday cake. The XXXXX in the title of this picture has been substituted for what may be the depicted girl's real name.

22. On March 14, 2011, I downloaded image files directly from Sisterskids. Among the files that I downloaded was a folder titled, "babies." Upon reviewing the downloaded image files, based on my training and experience, I believed that the majority of them depicted child pornography. Two of these files were matches to identified victims of child sexual exploitation. Results from an administrative subpoena sent to Comcast revealed that at the date and time of the downloads, the IP address of Sisterskids' computer was assigned to an account registered to D.H. at a known residential address in Cottage Grove, Minnesota.

23. On March 20 and March 23, 2011, I received information that the username Sisterskids was online. Results from an administrative subpoena sent to ICS Advanced Technologies revealed that on the dates and times Sisterskids was online, the IP address of Sisterskids' computer was assigned to a Microtel Inn and Suites in Ames, Iowa.

24. On March 30, 2011, SA Larsen served the Microtel Inn and Suites with a subpoena for registered guest information for March 19, 2011 through March 24, 2011. While in the parking lot of the Microtel Inn and Suites, SA Larsen observed two vehicles bearing Minnesota license plates, one of which was registered to STEVEN MICHAEL BORGAN, JR. of St. Paul, Minnesota.

25. I obtained a Minnesota Driver's license photograph for BORGAN and compared it to the image of the white male in the image "Me and my niece.jpg" that I had downloaded from Sisterskids on March 7, 2011. It is my belief that the male depicted in the image "Me and my niece.jpg" very closely resembles the image from BORGAN's Minnesota Driver's license.

28. On or about April 4, 2011, I used the online service Lexis Nexis to conduct a public records check for STEVEN BORGAN. The results of this check showed the following:

a. A date of birth of xx/xx/1980 and a Social Security Account number.

b. A listed address at an apartment in South St. Paul, Minnesota. On May 2, 2011, I received the results of a check for mail recipients at this address, which indicated that this is a vacant apartment previously occupied by BORGAN.

c. A potential relative with a listed address at the same known residential address in Cottage Grove, Minnesota corresponding to the Comcast account to which the IP address of Sisterskids' computer was assigned at the dates and times I downloaded child pornography from Sisterskids on March 14, April

19, May 5 and May 19, 2011. On May 2, 2011, I received the results of a check for mail recipients at this address, which included BORGAN's potential relative and several persons believed to be minors. One of these minors has the same first name as in the title of the picture "XXXXX birthday.bmp" that I downloaded from Sisterskids on March 7, 2011.

26. On or about April 4, 2011, I conducted an open source online search for the name "STEVEN BORGAN" and found the online profile <http://www.facebook.com/people/Steven-Borgan/10000052344483> on the social networking website www.facebook.com ("Facebook"). A picture on the main page for this profile appears to be identical to the picture titled "me.bmp" that I downloaded from Sisterskids on March 7, 2011.

27. I served Facebook with an administrative subpoena for this profile. In response, Facebook advised that it was registered in the name of STEVEN BORGAN, with an associated e-mail address of sborgan21@hotmail.com.

28. Facebook also provided logs listing the IP addresses that had been used to connect to this profile. Among these were several IP addresses that had been used by Sisterskids, including:

a. On November 5, 2010, this Facebook profile connected on the same day using the same Comcast IP address assigned to E.S. in Minneapolis Minnesota, that I downloaded child pornography images from Sisterskids.

b. On December 10, 2010, this Facebook profile connected on the same day using the same Mediacom IP address

assigned to C.N. in Boone, Iowa that I downloaded child pornography images from Sisterskids.

c. On January 28, 2011, this Facebook profile connected on the same day to the same Mediacom IP address assigned to A.D. in Boone, Iowa that SA Zajac downloaded child pornography images from Sisterskids.

d. On March 13, 2011, this Facebook profile connected using the same Comcast IP address assigned to D.H. in Cottage Grove, Minnesota that I downloaded images of child pornography from Sisterskids on March 14 and April 19, 2011.

e. On March 21, 2011, this Facebook profile connected using the IP address of the Microtel Inn and Suites in Ames, Iowa.

29. On April 19, 2011, May 5, 2011 and May 19, 2011, I downloaded image and video files directly from Sisterskids. Upon reviewing the downloaded image files, based on my training and experience, I believed that the majority of them depicted child pornography. Several of these files were matches to identified victims of sexual exploitation. Results from an administrative subpoena sent to Comcast revealed that on all three of these occasions, the IP address of Sisterskids' computer was assigned to an account registered to D.H. at the same known residential address in Cottage Grove, Minnesota as with regard to my March 14, 2011 download of child pornography from Sisterskids.

30. On April 21, 2011 and May 19, 2011, I conducted a physical surveillance of the known residential address in Cottage Grove, Minnesota and observed a red pickup truck with the same

license plate as the vehicle previously observed by SA Larsen at the Microtel Inn and Suites in Ames, Iowa and registered to STEVEN BORGAN, JR.

31. Between May 24, 2011 and June 6, 2011, I received information that the username Sisterskids was connecting to the publicly available peer-to-peer file sharing program from IP addresses which information subpoenaed from Qwest Communications showed resolved to Drake West Village at a known address in Des Moines, Iowa. During this same time period, BORGAN's vehicle was not observed in the vicinity of the known residential address in Cottage Grove, Minnesota.

32. On May 29, 2011, BORGAN's vehicle was observed to be parked in the vicinity of the Drake Village West apartments in Des Moines, Iowa.

33. On June 15, 2011, I downloaded image and video files directly from Sisterskids. Upon reviewing the downloaded image files, based on my training and experience, I believed that the majority of them depicted child pornography. The IP address of Sisterskids' computer at this date and time was one of the IP addresses that had previously been found to resolve to Drake West Village at a known address in Des Moines, Iowa.

34. On July 13, 2011, I used a computer connected to the Internet and launched the publicly available peer-to-peer file sharing program from the Minnesota Cyber Crime Task Force. I then connected to the file sharing program with a username that I had created and was indicative of a person with a sexual interest in

children. I then observed that the username Sisterskids was logged into the network at that time.

35. I then connected to and browsed the folders/directories being shared by Sisterskids and observed that this user was sharing approximately 16,731 files totaling approximately 73.62 GB of data.

36. I then downloaded 6 image files from Sisterskids. During the download of these files, I used a network monitoring program in order to identify the IP address of Sisterskids' computer, which was 24.118.100.208. Open source information showed this IP address to be registered to Comcast Communications.

37. I reviewed the downloaded image and files, and based on my training and experience, I believed that the majority of them depicted child pornography. Three of the files downloaded that depicted child pornography had the following names and are briefly described:

a. 0_10649900_1163577995.jpg

Image depicts a naked prepubescent girl with her legs opened and exposing her genitalia.

b. 1121732131663.jpg

Image depicts an adult male pulling aside the underwear of a prepubescent girl and exposing her genitalia. The male's penis is near the girl's genitalia.

c. baby cum.jpg

Image depicts a prepubescent girl with her legs spread and genitalia exposed. There is a penis near

the girl's genitalia, and there appears to be semen on the girl's stomach and chest.

38. Results from an administrative subpoena sent to Comcast for the date and time the above-noted files were downloaded revealed that IP address 24.118.100.208 was assigned to the account registered to D.H. at the same known residential address in Cottage Grove, Minnesota as with regard to my March 14, April 19, May 5 and May 19, 2011 downloads of child pornography from Sisterskids.

39. On July 14, 2011, at approximately 6:00 a.m. CDT, I conducted a physical surveillance at the known residential address in Cottage Grove, Minnesota. I observed the red pickup truck registered to STEVEN BORGAN, JR. parked in front of the residence.

40. On July 22, 2011, a federal search warrant was authorized by United States Magistrate Judge Jeffrey J. Keyes, which authorized the search of the residence in Cottage Grove, Minnesota associated with the IP address Sisterskids' computer was assigned at the dates and times I downloaded child pornography from Sisterskids on March 14, April 19, May 5, May 19 and July 13, 2011, and authorized the search of BORGAN's vehicle.

41. On July 25, 2011, at approximately 5:00 p.m., your affiant, other FBI agents and Cottage Grove police officers executed the search warrant at the residence in Cottage Grove, Minnesota and upon BORGAN's vehicle. Among the items seized from the residence were a Compaq laptop computer and other digital media, including external storage media.

42. At the time the search warrant was executed, BORGAN was present in the residence. Your affiant and other law enforcement conducted an interview with BORGAN at the scene. Initially, BORGAN denied having a computer. BORGAN ultimately admitted using Gigatribe, including the account with username "Sisterskids." BORGAN was shown screenshots of Sisterskids' shared folders on Gigatribe and identified them as folders he shared. In addition, BORGAN was shown copies of several child pornography images that were downloaded from Sisterskids, and he identified them as images he shared. BORGAN further admitted that he is sexually attracted to girls age 8 through teen.


43. In connection with the search warrant execution, an FBI computer forensic examiner conducted an on-scene preview of the laptop computer found in the residence and identified by BORGAN as his laptop computer. During the on-scene preview, law enforcement discovered approximately 6500 images that appeared to be child pornography because they depicted minors engaging in sexually explicit conduct. These images included the three child pornography images your affiant downloaded from Sisterskids on July 13, 2011: 0_10649900_1163577995.jpg, 1121732131663.jpg, and baby cum.jpg.

44. Following the conclusion of the interview with BORGAN and the on-scene preview of his laptop computer, BORGAN was placed under arrest.

45. Based upon these facts conveyed in this affidavit, your affiant believes that there is probable cause that, on or about

July 13, 2011, STEVEN MICHAEL BORGAN, JR. committed the offense of distribution of child pornography in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(b)(1).

Further your Affiant sayeth not.



ROBERT J. E. BLACKMORE
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 26th day of July, 2011.


JEFFREY J. KEYES
United States Magistrate Judge